

received by the host system. Before decrypting the DES communication, it must obtain the DES key and, accordingly, the host system 50 will issue, to one of the cryptosystems 10 a decryption request instruction, containing the encrypted DES key as the cyphertext C. If the (private) decryption keys,  $d, n$  (and its component primes,  $p_1, p_2, \dots, p_k$ ) are not held by the cryptosystem 10, they also will be delivered with the encryption request instruction.

In turn, the cryptosystem 10 would decrypt the received cyphertext in the manner described above (developing the sub-tasks, issuing the sub-tasks to the exponentiator 32 of the cryptosystem 10, and reassembling the results of the sub-task to develop the message data: the DES key), and return to the host system the desired, decrypted information.

Alternatively, the host system 50 may desire to deliver, via the communication medium 60, an encrypted communication to one of the stations 64. If the communication is to be encrypted by the DES scheme, with the DES key encrypted by the RSA scheme, the host system would encrypt the communication, forward the DES key to one of the cryptosystems 10 for encryption via the RSA scheme. When the encrypted DES key is received back from the cryptosystem 10, the host system can then deliver to one or more of the stations 64 the encrypted message.

Of course, the host system 50 and the stations 64 will be using the RSA scheme of public key encryption/decryption. Encrypted communications from the stations 64 to the host system 50 require that the stations 64 have access to the public key  $E$  ( $E, N$ ) while the host system maintains the private key  $D$  ( $D, N$ , and the constituent primes,  $p_1, p_2, \dots, p_k$ ). Conversely, for secure communication from the host system 50 to one or more of the stations 64, the host system would retain a public key  $E'$  for each station 64, while the stations retain the corresponding private keys  $E$ .

Other techniques for encrypting the communication could be used. For example, the communication could be entirely encrypted by the RSA scheme. If, however, the communication greater than  $n-1$ , it will need to be broken up into blocks size  $M$  where

40 ~~0 ≤ M ≤ n-1~~

Each block  $M$  would be separately encrypted/decrypted, using the public key/private key RSA scheme according to that described above.

45 What is claimed:

1. A method for establishing cryptographic communications comprising the step of:

50 encoding a plaintext message word  $M$  to a ciphertext word signal  $C$ , where  $M$  corresponds to a number representative of a message and

$$0 \leq M \leq n-1$$

55  $n$  being a composite number formed from the product of  $p_1 \cdot p_2 \cdot \dots \cdot p_k$  where  $k$  is an integer greater than 2,  $p_1, p_2, \dots, p_k$  are distinct prime numbers, and where  $C$  is a number representative of an encoded form of message word  $M$ , wherein said encoding step comprises the step of:

60 transforming said message word signal  $M$  to said ciphertext word signal  $C$  whereby

$$C = M^e \pmod{n}$$

65 where  $e$  is a number relatively prime to  $(p_1-1) \cdot (p_2-1)$ .

2. The method according to claim 1, comprising the further step of:

Sub  
A27  
B26

Sub  
A28  
B27

Sub  
A29  
B28

Sub  
A30  
B29

decoding the ciphertext word signal C to the message word signal M. wherein said decoding step comprises the step of: transforming said ciphertext word signal C. whereby:

$$M \equiv C^d \pmod{n}$$

where d is a multiplicative inverse of  $e \pmod{\text{lcm}((p_1-1), (p_2-1), \dots, (p_k-1))}$ .

3. A method for transferring a message signal  $M_i$  in a communications system having j terminals. wherein each terminal is characterized by an encoding key  $E_i = (e_i, n_i)$  and decoding key  $D_i = (d_i, n_i)$ , where  $i=1, 2, \dots, j$ , and wherein  $M_i$  corresponds to a number representative of a message-to-be-transmitted from the  $i^{\text{th}}$  terminal.  $n_i$  is a composite number of the form

$$n_i = p_{i,1} \cdot p_{i,2} \cdot \dots \cdot p_{i,k}$$

where k is an integer greater than 2.

$p_{i,1}, p_{i,2}, \dots, p_{i,k}$  are distinct prime numbers.

$e_i$  is relatively prime to  $\text{lcm}(p_{i,1}-1, p_{i,2}-1, \dots, p_{i,k}-1)$   $d_i$  is selected from the group consisting of the class of numbers equivalent to a multiplicative inverse of

$$e_i \pmod{\text{lcm}((p_{i,1}-1), (p_{i,2}-1), \dots, (p_{i,k}-1))},$$

comprising the step of:

encoding a digital message word signal  $M_A$  for transmission from a first terminal ( $i=A$ ) to a second terminal ( $i=B$ ). said encoding step including the sub-step of:

transforming said message word signal  $M_A$  to one or more message block word signals  $M_A''$ . each block word signal  $M_A''$  corresponding to a number representative of a portion of said message word signal  $M_A$  in the range  $0 \leq M_A'' \leq n_B - 1$ .

transforming each of said message block word signals  $M_A''$  to a ciphertext word signal  $C_A$ .  $C_A$  corresponding to a number representative of an encoded form of said message block word signal  $M_A''$ . whereby:

$$C_A \equiv M_A''^{e_B} \pmod{n_B}.$$

4. A cryptographic communications system comprising: a communication medium:

an encoding means coupled to said channel and adapted for transforming a transmit message word signal M to a ciphertext word signal C and for transmitting C on said channel. where M corresponds to a number representative of a message and

$0 \leq M \leq n-1$  where n is a composite number of the form

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_k$$

where k is an integer greater than 2 and  $p_1, p_2, \dots, p_k$  are distinct prime numbers. and where C corresponds to a number representative of an enciphered form of said message and corresponds to

$$C \equiv M^e \pmod{n}$$

where e is a number relatively prime to  $\text{lcm}(p_1-1, p_2-1, \dots, p_k-1)$ ; and

a decoding means coupled to said channel and adapted for receiving C from said channel and for transforming C to a receive message word signal M' where M' corre-

sponds to a number representative of a deciphered form of C and corresponds to

$$M' \equiv C^d \pmod{n}$$

5 where d is selected from the group consisting of the class of numbers equivalent to a multiplicative inverse of

$$e \pmod{\text{lcm}((p_1-1), (p_2-1), \dots, (p_k-1))}.$$

10 5. A cryptographic communications system having a plurality of terminals coupled by a communications channel, including a first terminal characterized by an associated encoding key  $E_A=(e_A, n_A)$  and decoding key  $D_A=(d_A, n_A)$ , wherein  $n_A$  is a composite number of the form

$$n_A = p_{A,1} \cdot p_{A,2} \cdot \dots \cdot p_{A,k}$$

where k is an integer greater than 2,  $p_{A,1}, p_{A,2}, \dots, p_{A,k}$  are distinct prime numbers,  $e_A$  is relatively prime to

$$20 \quad \text{lcm}(p_{A,1}-1, p_{A,2}-1, \dots, p_{A,k}-1)$$

$d_A$  is selected from the group consisting of the class of numbers equivalent to a multiplicative inverse of

$$25 \quad e_A \pmod{\text{lcm}((p_{A,1}-1), (p_{A,2}-1), \dots, (p_{A,k}-1))},$$

and including a second terminal, comprising:

blocking means for transforming a message-to-be-transmitted from said second terminal to said first terminal to one or more transmit message word signals  $M_B$ , where  $M_B$  corresponds to a number representative of said message in the range

$$35 \quad 0 \leq M_B \leq n_A - 1.$$

encoding means coupled to said channel and adapted for transforming each transmit message word signal  $M_B$  to a ciphertext word signal  $C_B$  and for transmitting  $C_B$  on said channel.

40 where  $C_B$  corresponds to a number representative of an enciphered form of said message and corresponds to

$$C_B \equiv M_B^{e_A} \pmod{n_A}$$

45 wherein said first terminal comprises:

decoding means coupled to said channel and adapted for receiving said ciphertext word signals  $C_B$  from said channel and for transforming each of said ciphertext word signals to a receive message word signal  $M_B$ , and means for transforming said receive message word signals  $M'$  to said message, where  $M'$  is a number representative of a deciphered form of  $C_B$  and corresponds to

$$55 \quad M_B' \equiv C_B^{d_A} \pmod{n_A}.$$

6. The system according to claim 5 wherein said second terminal is characterized by an associated encoding key  $E_B=(e_B, n_B)$  and decoding key  $D_B=(d_B, n_B)$ , where:

60  $n_B$  is a composite number of the form

$$n_B = p_{B,1} \cdot p_{B,2} \cdot \dots \cdot p_{B,k}$$

where k is an integer greater than 2,  $p_{B,1}, p_{B,2}, \dots, p_{B,k}$  are distinct prime numbers,  $e_B$  is relatively prime to

$$65 \quad \text{lcm}(p_{B,1}-1, p_{B,2}-1, \dots, p_{B,k}-1).$$

$d_B$  is selected from the group consisting of the class of numbers equivalent to a multiplicative inverse of

$$e_B(\text{mod lcm}((p_{B,1}), (p_{B,2}-1), \dots, (p_{B,k}-1))).$$

5

wherein said first terminal comprises:

blocking means for transforming a message-to-be-transmitted from said first terminal to said second terminal, to one or more transmit message word signals  $M_A$ , where  $M_A$  corresponds to a number representative of said message in the range

$$0 \leq M_A \leq n_B(\text{mod } n_B)$$

encoding means coupled to said channel and adapted for transforming each transmit message word signal  $M_A$  to a ciphertext word signal  $C_A$  and for transmitting  $C_A$  on said channel.

15

where  $C_A$  corresponds to a number representative of an enciphered form of said message and corresponds to

20

$$C_A \equiv M_A^{e_B}(\text{mod } n_B)$$

wherein said second terminal comprises;

decoding means coupled to said channel and adapted for receiving said ciphertext word signals  $C_A$  from said channel and for transforming each of said ciphertext word signals to a receive message word signal  $M'_A$ , and means for transforming said receive message word signals  $M'_A$  to said message.

25

where  $M'$  corresponds to a number representative of a deciphered form of  $C$  and corresponds to

30

$$M_A \equiv C_A^{d_B}(\text{mod } n_B).$$

7. A method for establishing cryptographic communications comprising the step of:

35

encoding a digital message word signal  $M$  to a cipher text word signal  $C$ , where  $M$  corresponds to a number representative of a message and

40

$$0 \leq M \leq n-1,$$

where  $n$  is a composite number having at least 3 whole number factors greater than one, the factors being distinct prime numbers, and

45

where  $C$  corresponds to a number representative of an encoded form of message word  $M$ .

wherein said encoding step comprises the step of:

transforming said message word signal  $M$  to said ciphertext word signal  $C$  whereby

50

$$C \equiv eM^e + a_{e-1}M^{e-1} + \dots + a_0(\text{mod } n)$$

where  $e$  and  $a_{e-1}, a_{e-2}, \dots, a_0$  are numbers.

55

8. In the method according to claim 7 where said encoding step includes the step of transforming  $M$  to  $C$  by the performance of a first ordered succession of invertible operations on  $M$ , the further step of:

decoding  $C$  to  $M$  by the performance of a second ordered succession of invertible operations on  $C$ , where each of the invertible operations of said second succession is the inverse of a corresponding one of said first succession, and wherein the order of said operations in said second succession is reversed with respect to the order of corresponding operations in said first succession.

65

9. A communication system for transferring message signals  $M_i$ , comprising:

$j$  stations, each of the  $j$  stations being characterized by an encoding key  $E_i=(e_i, n_i)$  and decoding key  $D_i=(d_i, n_i)$ , where  $i=1, 2, \dots, j$ , and wherein

$M_i$  corresponds to a number representative of a message signal to be transmitted from the  $i^{\text{th}}$  terminal, and

$$0 \leq M_i \leq n_i - 1,$$

$n_i$  is a composite number of the form

$$n_i = p_{i,1} \cdot p_{i,2} \cdot \dots \cdot p_{i,k}$$

where  $k$  is an integer greater than 2.

$p_{i,1}, p_{i,2}, \dots, p_{i,k}$  are distinct prime numbers.

$e_i$  is relatively prime to  $\text{lcm}(p_{i,1}-1, p_{i,2}-1, \dots, p_{i,k}-1)$ .

$d_i$  is selected from the group consisting of the class of numbers equivalent to a multiplicative inverse of

$$e_i \pmod{(\text{lcm}(p_{i,1}-1, p_{i,2}-1, \dots, p_{i,k}-1))};$$

a first one of the  $j$  terminals including

means for encoding a digital message word signal

$M_A$  for transmission from said first terminal

( $i=A$ ) to a second one of the  $j$  terminals ( $i=B$ ),

and

means for transforming said message word signal

$M_A$  to a signed message word signal  $M_{A,s}$ ,  $M_{A,s}$

corresponding to a number representative of an

encoded form of said message word signal  $M_A$ ,

whereby:

$$M_{A,s} \equiv M_A^{e_A} \pmod{n_A}.$$

10. The system of claim 9 further comprising:

means for transmitting said signal message word signal

$M_{A,s}$  from said first terminal to said second terminal,

and wherein said second terminal includes means for

decoding said signed message word signal  $M_{A,s}$  to said

message word signal  $M_A$ , said second terminal including:

means for transforming said signed message word

signal  $M_{A,s}$  to said message word signal  $M_A$ ,

whereby

$$M_A \equiv M_{A,s}^{d_A} \pmod{n_A}.$$

11. A communications system for transferring a message signal  $M_i$ , the communications system comprising

$j$  communication stations each characterized by an encoding

key  $E_i=(e_i, n_i)$  and decoding key  $D_i=(d_i, n_i)$ , where

$i=1, 2, \dots, j$ , and wherein  $M_i$  corresponds to a number

representative of a message signal to be transmitted

from the  $i^{\text{th}}$  terminal,  $n_i$  is a composite number of the

form

$$n_i = p_{i,1} \cdot p_{i,2} \cdot \dots \cdot p_{i,k}$$

where

$k$  is an integer greater than 2.

$p_{i,1}, p_{i,2}, \dots, p_{i,k}$  are distinct prime numbers.

$e_i$  is relatively prime to  $\text{lcm}(p_{i,1}-1, p_{i,2}-1, \dots, p_{i,k}-1)$ .

$d_i$  is selected from the group consisting of the class of numbers equivalent to a multiplicative inverse of

$$e_i(\text{mod}(\text{lcm}((p_{i,1}-1), (p_{i,2}-1), \dots, (p_{i,j}-1))))$$

a first one of the  $j$  communication stations including  
 means for encoding a digital message word signal  $M_A$   
 for transmission from said first one of the  $j$  commu- 5  
 nication stations ( $i=A$ ) to a second one of the  $j$   
 communication stations ( $i=B$ ).  
 means for transforming said message word signal  $M_A$   
 to one or more message block word signals  $M_A''$ ,  
 each block word signal  $M_A''$  being a number repre- 10  
 sentative of a portion of said message word signal  
 $M_A$  in the range  $0 \leq M_A'' \leq n_B - 1$ , and  
 means for transforming each of said message block  
 word signals  $M_A''$  to a ciphertext word signal  $C_A$ .  $C_A$  15  
 corresponding to a number representative of an  
 encoded form of said message block word signal  
 $M_A''$ , whereby:

$$C_A \equiv M_A''^{EB} (\text{mod } n_B).$$

12. The system of claim 11 further comprising: 20

means for transmitting said ciphertext word signals from  
 said first terminal to said second terminal, and  
 wherein said second terminal includes means for decod-  
 ing said ciphertext word signals to said message word 25  
 signal  $M_A$ , said second terminal including:  
 means for transforming each of said ciphertext word  
 signals  $C_A$  to one of said message block  
 word signals  $M_A''$ , whereby

$$M_A'' = C_A^{D_A} \pmod{n_A}$$

means for transforming said message block word signals  $M_A''$  to said message word signal  $M_A$ .

13. In a communications system, including first and second communicating stations interconnected for communication therebetween,

the first communicating station having

10 encoding means for transforming a transmit message word signal  $M$  to a ciphertext word signal  $C$  where  $M$  corresponds to a number representative of a message and

$$15 \quad 0 \leq M \leq n-1$$

where  $n$  is a composite number having at least 3 whole number factors greater than one, the factors being distinct prime numbers, and

20 where  $C$  corresponds to a number representative of an enciphered form of said message and corresponds to

$$C = eM^e + a_{e-1}M^{e-1} + \dots + a_0 \pmod{n}$$

25 where  $e$  and  $a_{e-1}, a_{e-2}, \dots, a_0$  are numbers; and means for transmitting the ciphertext word signal  $C$  to the second communicating station.

\* \* \* \* \*

Ins.  
B30